UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

MOHAMED OSMAN MOHAMUD,

Defendant.

Criminal Case No. 3:10-CR-00475-KI

OPINION AND ORDER

S. Amanda Marshall
United States Attorney
District of Oregon
Ethan D. Knight
Jolie F. Zimmerman
Assistant United States Attorneys
1000 SW Third Avenue, Suite 600
Portland, Oregon 97204

Attorneys for Plaintiff

Steven T. Wax
Federal Public Defender
Stephen R. Sady
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, Oregon 97204

Attorneys for Defendant

KING, Judge:

Defendant Mohamed Osman Mohamud is charged with attempting to use a weapon of mass destruction, specifically a destructive device or explosive bomb, against a person or property within the United States, in violation of 18 U.S.C. § 2332a(a)(2)(A). On November 29, 2010, the government filed a FISA Notification which gave Mohamud notice that the government intended to offer into evidence, or otherwise use or disclose in the case's proceedings, information obtained and derived from electronic surveillance and a physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, 50 U.S.C. §§ 1801-1812, 1821-1829. Before the court is Mohamud's Motion to Disclose FISA-Related Material Necessary to Litigate Motions for Discovery and for Suppression of the Fruits of FISA Activity [54]. I deny the motion for the reasons explained below.

DISCUSSION

Mohamud asks the court to: (1) disclose all FISA warrants, applications, and their fruits to defense counsel under the FISA provision calling for disclosure of information to an aggrieved person when necessary for litigation or pretrial motions or when required by due process; (2) review the FISA warrants under a de novo standard; (3) suppress all evidence and fruits of the evidence obtained through FISA, if the government violated any FISA provisions; and (4) find

FISA unconstitutional under any of several theories and suppress all evidence and fruits of the evidence obtained through FISA.

The government asks the court to: (1) conduct an in camera, ex parte review of the FISA dockets and the government's classified submission; (2) hold that the FISA surveillance was lawfully authorized and lawfully conducted in compliance with the Fourth Amendment; (3) hold that disclosure to the defense of the FISA dockets and the government's classified submissions is not required because the court can make an accurate determination of the legality of the surveillance without disclosure; (4) find FISA constitutional; and (5) order the Classified Information Security Officer to maintain the FISA dockets and the government's classified submissions under seal.

I. Overview of FISA

FISA provides a procedure for the executive branch to obtain judicial orders allowing electronic surveillance or physical searches when a significant purpose of the requested surveillance is to obtain foreign intelligence information. United States v. Abu-Jihaad, 630 F.3d 102, 117-119 (2nd Cir. 2010) (FISA's "significant purpose" requirement does not violate the Fourth Amendment), cert. denied, 131 S. Ct. 3062 (2011).

FISA requires the Chief Justice to designate eleven United States District Judges to sit as judges of the Foreign Intelligence Surveillance Court ("FISC") to consider ex parte applications for electronic surveillance and physical searches when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. 50 U.S.C. § 1803(a)(1). The Chief Justice also designates three United States District or Circuit Judges to sit on a court to review denials of FISA applications. 50 U.S.C. § 1803(b).

The parties agree that Mohamud is a "United States person" as defined by FISA, and is thus entitled to certain additional protections. 50 U.S.C. § 1801(i).

FISA defines "Foreign intelligence information" as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> >
> > (C) clandestine intelligence activities . . . ; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
>
> > (A) the national defense or the security of the United States; or
> >
> > (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e).[1]

A. FISA Applications

To obtain an order to conduct electronic surveillance under FISA, a federal officer must apply to one of the FISC judges. The Attorney General must approve each application "based upon his finding that it satisfies the criteria and requirements" of FISA. 50 U.S.C. § 1804(a). The application must include:

(1) the identity of the Federal officer making the application;

---

[1] I will generally cite only to the portion of FISA which pertains to electronic surveillance, 50 U.S.C. §§ 1801-1812. For the most part, there are similar provisions in the portions of FISA which pertain to physical searches, 50 U.S.C. §§ 1821-1829. The differences are not relevant to the analysis.

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that–

> (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
>
> (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures;

(5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification or certifications [from one of a list of high-ranking executive branch officials with national security responsibilities]–

> (A) that the certifying official deems the information sought to be foreign intelligence information;
>
> (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
>
> (E) including a statement of the basis for the certification that–
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques;

> (7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;
>
> (8) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and
>
> (9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.

50 U.S.C. § 1804(a).

FISA requires minimization procedures, defined as:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information[.]

50 U.S.C. § 1801(h)(1).

FISA allows evidence of a crime to be retained, with minimization procedures also including "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h)(3).

B. FISA Orders

A FISC judge enters an ex parte order approving an application only if the judge finds:

(1) the application was made by a federal officer and approved by the Attorney General;

(2) there is probable cause to believe "(A) the target of the electronic surveillance is a foreign

power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;" (3) the proposed minimization procedures meet FISA's requirements; and (4) the application contains all statements and certifications required by FISA and, if the target is a United States person, the certification or certifications are not clearly erroneous. 50 U.S.C. § 1805(a). In deciding whether probable cause exists, the FISC judge "may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. § 1805(b).

A FISA order must specify: (1) the identity, if known, or a description of the specific target; (2) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known; (3) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance; (4) the means by which the electronic surveillance will be effected and whether physical entry will be used; and (5) the time period during which the electronic surveillance is approved. 50 U.S.C. § 1805(c)(1). Moreover, the order must direct that the minimization procedures be followed. 50 U.S.C. § 1805(c)(2)(A). FISA orders can approve electronic surveillance and physical searches targeting a United States person for up to 90 days. 50 U.S.C. § 1805(d)(1). The FISC judge may assess compliance with the minimization procedures at or before the end of the approved time period. 50 U.S.C. § 1805(d)(3).

C. Judicial Review of FISA Orders

An aggrieved person may move to suppress evidence obtained under a FISA order on two grounds: (1) the information was unlawfully acquired under FISA; or (2) the surveillance was not performed in conformity with the FISA order. 50 U.S.C. § 1806(e).

Attorney General Eric H. Holder, Jr., filed a Declaration and Claim of Privilege in which he states that "it would harm the national security of the United States to disclose or hold an adversarial hearing with respect to the FISA Materials." Holder Decl. ¶ 3, filed as Government's Am. Unclassified Mem. in Opp'n to Def.'s Mot. to Disclose FISA-Related Material, ECF No. 88, Ex. 1.

If an aggrieved person files a motion to suppress or to obtain FISA applications or orders or evidence obtained through FISA orders, and the Attorney General files a declaration stating that disclosure or an adversary hearing would harm the national security of the United States, the district court shall

> review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

50 U.S.C. § 1806(f).

Thus, the court cannot make a disclosure to defendant unless the court first concludes that the government's filed materials are inadequate for the court to make an "accurate determination" of whether the FISA order was correctly obtained and the surveillance was in accord with the order. "[D]isclosure of FISA materials is the exception and *ex parte, in camera*

determination is the rule." Abu-Jihaad, 630 F.3d at 129 (internal quotation omitted); United States v. el-Mezain, 664 F.3d 467, 567 (5th Cir. 2011) (same, quoting Abu-Jihaad). The court is unaware of, and Mohamud has not directed me to, any case in which a court granted a defense motion to disclose FISA applications and orders.

If the district court "determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." 50 U.S.C. § 1806(g).

II. Constitutionality of FISA

A. Patriot Act of 2001 Amendments to FISA

Mohamud contends that FISA, as amended by the Patriot Act, violates the Fourth Amendment's prohibition on unreasonable searches and seizures. Further, Mohamud argues that even prior to the amendment, FISA violates the Fourth Amendment unless it is interpreted to require that the primary purpose of the surveillance is to obtain foreign intelligence information.

As originally written in 1978, FISA required a national security officer to certify that "the purpose" of the surveillance is to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(7)(B) (pre-2001 versions). Several circuits followed a pre-FISA case, United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980), to read a "primary purpose" requirement into this language. See In re: Sealed Case, 310 F.3d 717, 725-728 (FISA Ct. Rev. 2002) (explaining history of the primary purpose test). The Patriot Act of 2001 amended FISA, changing "the purpose" to "a significant purpose." USA Patriot Act of 2001, Pub. L. 107-56, § 218, 115 Stat. 291.

In Sealed Case, the FISA Court of Review addressed whether the Patriot Act amendment to FISA violated the Fourth Amendment. The court first held that, prior to the amendment, FISA "did *not* preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution." Sealed Case, 310 F.3d at 727. This conclusion undermined the holdings of several courts of appeals that FISA could only be used if, in pursuing foreign intelligence information, the government's primary purpose was not for a criminal prosecution. Id. at 722. The FISA Court of Review went on to consider the constitutionality of the Patriot Act amendment, which imposed the "significant purpose" requirement on obtaining foreign intelligence. The court compared FISA procedures with procedures to obtain an ordinary criminal wiretap under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-22. It also considered the "underlying rationale of the primary purpose test" which other courts had imposed as a constitutional requirement. Id. at 742. After a lengthy analysis, the court held:

> [W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from [United States v. United States District Court (Keith), 407 U.S. 297, 92 S. Ct. 2125, 2139 (1972)], that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

Id. at 746.

Numerous other courts have held that FISA's significant purpose requirement does not violate the Fourth Amendment. Abu-Jihaad, 630 F.3d at 128; El-Mezain, 664 F.3d at 568-70; United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005).

I see no error in these analyses and adopt the holding that the "significant purpose" requirement in FISA does not violate the Fourth Amendment.

B. Other Constitutional Issues

Mohamud notes that FISA provides for the disclosure of FISA materials to the extent due process requires. 50 U.S.C. § 1806(g). He claims that the ex parte FISA procedures violate due process, his right to be present at all critical stages of the criminal process, and his right to the effective assistance of counsel.

Numerous courts have held that FISA's ex parte proceedings do not violate a defendant's due process rights. United States v. Ott, 827 F.2d 473, 476-77 (9th Cir. 1987) (due process not violated by court's reliance on Attorney General's affidavit based on sealed exhibits, by lack of disclosure to defense counsel who had security clearances, or by failure to provide more liberal discovery normally permitted in military context); Abu-Jihaad, 630 F.3d at 129; El-Mezain, 664 F.3d at 566-68 (balancing test in Mathews v. Eldridge, 424 U.S. 319, 96 S. Ct. 893 (1976), does not require disclosure of FISA materials because the court's ex parte review adequately assured that defendant's constitutional rights were not violated and, as a matter of national security, the government has a substantial interest in maintaining the secrecy of the materials); Damrah, 412 F.3d at 624 (defendant's reliance on Mathews to argue that the Due Process Clause requires an evidentiary hearing is misplaced because FISA's requirement that the district court conduct an ex parte review of FISA materials does not deprive a defendant of due process).

Mohamud's defense counsel provided me with ex parte filings in which they explain some of the theories of the defense. This information allows me to make better determinations of whether a particular piece of information might be exculpatory and discoverable under Brady. I

am not persuaded that due process requires disclosure of the materials here, even in light of the circumstances in Mohamud's case.

The District of Columbia Circuit analyzed the argument that FISA's failure to require disclosure and an adversary hearing violates a defendant's Fifth and Sixth Amendment rights. The court reasoned that FISA is concerned with foreign intelligence surveillance.

> The statute is meant to reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights. In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.

United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982) (internal quotation omitted). I am unpersuaded that the Patriot Act amendments undermine the holding in Belfield. FISA still requires that a significant purpose of the surveillance is to obtain foreign intelligence.

I am also unpersuaded that the judiciary must defer to the executive branch during a FISA ex parte review to the extent that the constitutional separation of powers is violated. United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987) (FISA's probable cause requirements provide ample judicial scrutiny of the government's need for the intelligence information).

Mohamud also contends the FISA applications "may" contain intentional or reckless material falsehoods or omissions significant enough for the surveillance to violate the principles in Franks v. Delaware, 438 U.S. 154 (1978). Mohamud claims this argument is sufficient to entitle him to a Franks hearing so he can inquire into the affiant's statements on the FISA applications.

In Franks, the Supreme Court held that, under certain circumstances, a defendant is entitled to an evidentiary hearing in which he can attack the veracity of a search warrant affidavit or challenge the omission of material facts in the affidavit. When a defendant seeks a Franks hearing because of "allegations of material false statements or omissions in an affidavit supporting a search warrant, a defendant must make a substantial preliminary showing that false or misleading statements were (1) deliberately or recklessly included in an affidavit submitted in support of a search warrant; and (2) necessary to the finding of probable cause." United States v. Flyer, 633 F.3d 911, 916 (9th Cir. 2011) (internal quotations omitted).

Because Mohamud has not seen the FISA applications, he can only speculate that there may be false statements or omissions. This is insufficient to qualify as a substantial preliminary showing. I realize the difficult position Mohamud's defense team is in, but the denial of a Franks hearing is commonplace and acceptable in the FISA context. See El-Mazain, 664 F.3d at 570; Damrah, 412 F.3d at 624-25; Abu-Jihaad, 630 F.3d at 130.

III. Review of FISA Applications and Orders

A. Standard of Review

The first issue is to determine the appropriate standard of review. Courts are split–some apply a deferential standard to the FISC's probable cause determinations and others perform a de novo review. United States v. Hammoud, 381 F.3d 316, 332 (4th Cir. 2004), rev'd on other grounds, 543 U.S. 1097, opinion reinstated in pertinent part, 405 F.3d 1034 (4th Cir. 2005) (de novo); Abu-Jihaad, 630 F.3d at 130 (deferential). Without deciding the issue, I will make a de novo review.

FISA expressly obliges the court to give more deference to the certifications; "if the target is a United States person, [the court should ensure] the certification or certifications are not clearly erroneous." 50 U.S.C. § 1805(a).

Concerning minimization, "Congress recognized that 'no electronic surveillance can be so conducted that innocent conversations can be totally eliminated.'" Hammoud, 381 F.3d at 334 (quoting S. Rep. No. 95-701, at 39 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 4008). The test is whether the government made "a good faith effort to minimize the acquisition and retention of irrelevant information." Id.

B. Results of the Court's Ex Parte Review

The court made a careful de novo ex parte review of the FISA applications and draws the following conclusions: (1) the applications contain all of the required information, as specified in 50 U.S.C. § 1804(a); (2) the applications contain the required certifications from an appropriate high-ranking official of the United States government, and the certifications are not clearly erroneous; (3) the applications contain sufficient information to support the FISC's probable cause determinations; and (4) the proposed minimization procedures meet FISA's requirements. I find that the FISA surveillance was lawfully authorized by the FISC.

I also find that the government agents followed appropriate minimization procedures and conducted the surveillance within the time periods authorized by the FISA orders. Thus, I conclude the FISA surveillance was lawfully conducted.

C. The Court's Ability to Make an Accurate Determination of Legality

Mohamud argues several reasons why this court cannot make an accurate determination of the legality of the FISA surveillance without the assistance of defense counsel after disclosure of the FISA applications and orders to the defense.

– Mohamud claims there are complex questions concerning whether he, as a United States person, fits within the FISA definition of an agent of a foreign power and that definition's relationship to criminal activity.

– Because Mohamud became 18 years old on August 11, 2009, he contends that any surveillance prior to that date creates additional issues concerning the reasonableness of the surveillance.

– Noting the discovery the government provided to the defense includes material Mohamud read and wrote, he argues defense counsel's assistance is necessary to enforce the protection of his First Amendment rights expressly contained in FISA.

– Mohamud claims defense involvement is needed to assist the court in determining if the applications met FISA's necessity requirement.

– Mohamud is concerned that the apparent breadth of the surveillance raises potential minimization problems which require defense involvement to properly address.

– Mohamud notes federal agents' involvement in the November 2009 state investigation into unfounded allegations of his sexual misconduct. He argues that without disclosure of the FISA materials, the defense cannot evaluate causation regarding state actions or any taint arising from searches going beyond his consent.

– Due to the length of the surveillance, Mohamud contends that the defense must examine all FISA orders to determine if there were any lapses of time between extensions and whether extensions were all obtained under appropriate FISA procedures.

– Mohamud speculates that the FISA applications may contain intentional or reckless material falsehoods or omissions and that the surveillance thus may violate the principles of Franks v. Delaware, 438 U.S. 154 (1978).

The government claims that most of these factors are present in any court's review of FISA applications and orders and, thus, this court is qualified to perform the ex parte review without the assistance of defense counsel. I generally agree, but assure Mohamud that I kept his arguments in mind during my review of the FISA materials. Moreover, I saw nothing during the review that gave me cause for concern that false statements were made to support the FISA application materials. I cannot comment on the content of the FISA applications, but note that they were well-supported in great detail. I see no basis for a Franks hearing.

CONCLUSION

Mohamud's Motion to Disclose FISA-Related Material Necessary to Litigate Motions for Discovery and for Suppression of the Fruits of FISA Activity [54] is denied.

IT IS SO ORDERED.

Dated this 7th day of May, 2012.

/s/ Garr M. King
Garr M. King
United States District Judge